SmartOn®

ICカード認証ソリューション

スマートオン

ICカードとパスワードで本人認証し、セキュリティを強化
PC不正利用を事前に防止し、大切な情報を守る

- PC利用時の「本人認証」をICカードを使って強化
- 様々なシンクライアント環境にも対応
- ユーザーに適切な情報アクセス環境を提供
- Webサイトやアプリケーションに自動ログオンが可能
- 組織に最適なシステム構成で、継続的な運用を実現

株式会社富士キメラ総研
「2004~2013
ネットワークセキュリティビジネス調査総覧」
デバイス認証ツール市場における
調査結果より

セキュリティの

セキュリティを一つ上のレベルに引き上げるもの。それはログ
PCを使う人が、本当にそのPCで利用して良い人であるか、そのPCを利用している人は
SmartOnはICカードを利用し、「本人しか知らないパスワード」と「本人しか持って

SmartOnは、1997年に販売を開始し、3000社以上のお客様にご利用いただいている製品です。多くの実績により、お客様の声を反映した様々な運用が可能な設計になっています。

課題01 なりすまし

パスワードだけで認証を行っていると、本人になりすまして不正にPCを利用されてしまう可能性がある。パスワード漏洩はセキュリティの根底を揺るがしかねない。

課題04 パスワードが多すぎる

Webサイトやクラウドサービスなど利用システムが増え、覚えるパスワードが増加。定期的なパスワード変更がユーザーや管理者の負担になっている。

課題02 PCの持ち出し

PCの紛失・盗難にあった時、パスワードだけの認証では突破されてしまう可能性がある。モバイルPCでも安全に持ち出せるようにしたい。

課題05 PCの私的利用

アプリやPCリソースを自由に使わせておくと、勝手な設定変更でPCの不具合や無駄な問合せにつながる。不正ソフトや不正USBの利用は防ぎたい。

課題03 仮想デスクトップへの認証

PCをシンクライアント化するとデータをPC上に置かなくて済むが、パスワードだけでデータへアクセス出来てしまうのは心配。

課題06 ログの信憑性

共有PCで共通のWindowsアカウントを利用している場合、実際に誰が利用しているのかわからない。

全ては認証から

オンしている人が本人であるという「本人認証」を行う事です。
本当に本人であるか、パスワードだけではこれらを確実なものにするのは不可能です。
いないICカード」を使ってPCにログオンすることで、「本人認証」を確実なものにします。

解決01 ICカード+パスワードでの認証

本人であると証明する要素として、ICカードを追加。二要素（ICカードとパスワード）で認証を行うことにより、なりすましを防止し、セキュリティが大幅に向上します。

➡P.4

解決04 シングルサインオン

ユーザーに変わってICカードがパスワードを記憶します。ユーザーはパスワードを覚える必要が無くなるので、パスワードの漏洩がなくなり、セキュリティ・業務効率の両方が向上します。

➡P.5

解決02 モバイルPCの認証強化

持ち歩くPCこそ認証を強化する必要があります。PCが紛失・盗難にあっても、ICカードが無ければPCを利用できません。これが二要素認証の最大の強みです。

➡P.4

解決05 アプリ・USBメモリ・PCリソースの制御

ユーザー毎にアプリやUSBメモリ等の利用を制御することで、業務に不必要な操作を禁止し、事故を防ぎ、ユーザー・管理者共に業務効率が上がります。

➡P.5

解決03 混在環境でもOK!

仮想デスクトップへのアクセスも認証強化することでセキュリティを向上。通常PC・シンクライアントの混在環境でも1システムで管理可能です。

➡P.4

解決06 ユーザーに紐付く確かなログ

ユーザーに紐づいたカードで認証をするので、Windowsアカウントが1つでも、誰が利用しているのかわかります。

➡P.6

ICカードでPCセキュリティを強化

SmartOn Logon

ICカード+パスワードによる確実な本人認証

ICカードが発行されたユーザーだけにPCの利用を許可し、なりすましを防ぎます。

LOCK

カードリーダーにICカードをかざし、
表示されるログイン画面でパスワードを入力。

パスワード認証に成功すると
Windowsにログオン。

カードリーダーからICカードをは外すと
PCをロック。

ログオン画面のSmartOnロゴはオリジナルのデザインに変更が可能です。ログオンの際に、下記項目を組み合わせることができます。

- SmartOnパスワード
- Windowsアカウント
- Windowsパスワード

ログオンしたユーザーによって利用権限を制御できます。

カードを外した時の動きが選べます。

認証後のセキュリティも確保

少しの間でも離席する際、PCをロックしないと、悪意のある第三者にPCを操作されてしまいます。せっかく本人認証をしても、これでは意味がありません。SmartOnは、カードを持って離れるだけで簡単にPCをロックできるので、ユーザーにロックの操作を教える事もありません。「カードを持って席を立つ」これだけで大丈夫です。

SmartOn未導入

ロックをしないと
ログオンしたまま

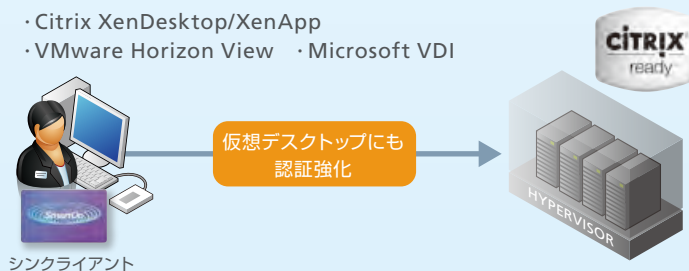
SmartOn導入後

カードを持って
離れるだけでロック

仮想デスクトップにも対応

仮想デスクトップ環境でも二要素認証が可能です。通常PC・シンクライアントの一元管理が可能なので、段階的にシンクライアント環境への移行が可能です。

- SmartOnは、主要仮想デスクトップ製品に対応しています。
  - ・Citrix XenDesktop/XenApp
  - ・VMware Horizon View　・Microsoft VDI

CiTRiX ready

いろいろなICカードが使えます

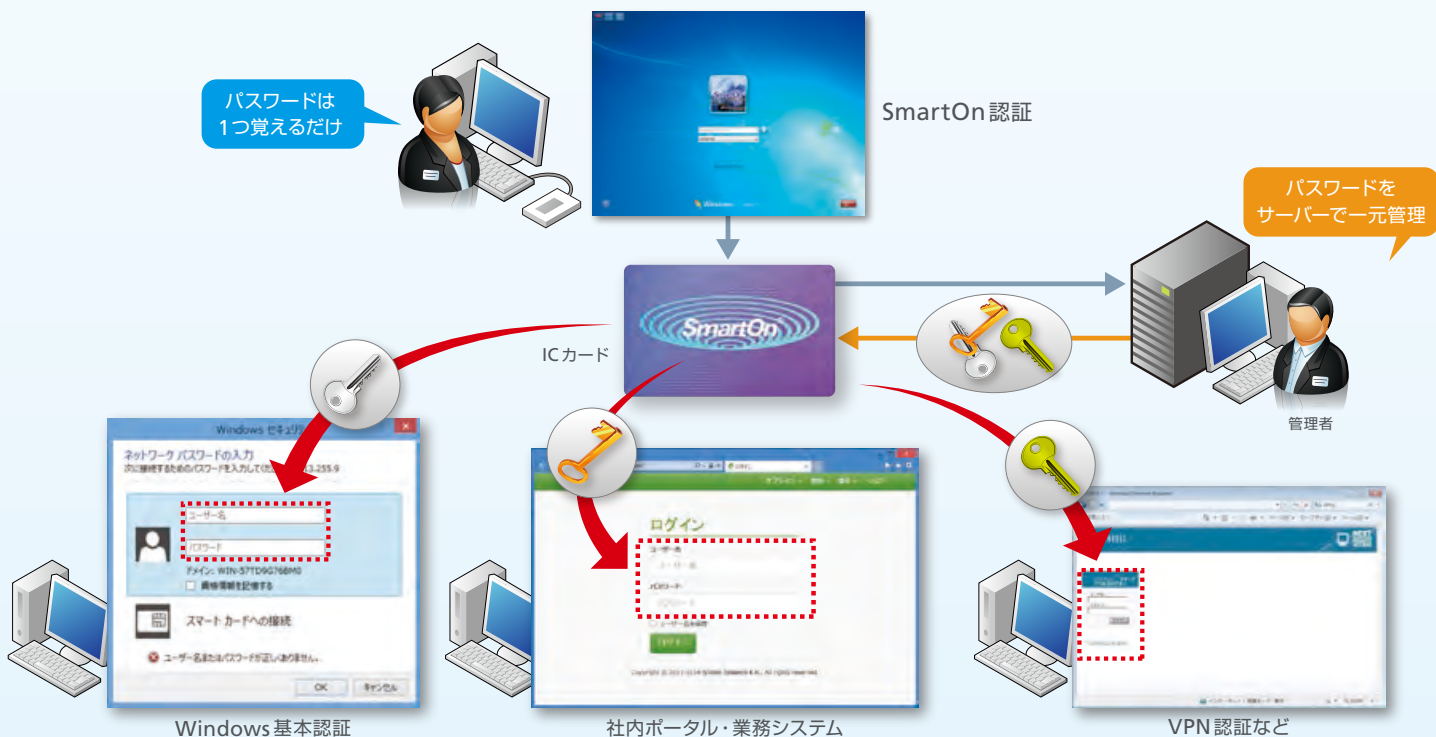
社員証や入退室、プリンタ認証システムなどで既に利用しているICカード※1を活用して、認証システムを構築できます。

- FeliCa（フェリカ）
  - ・交通系カード
  - ・FeliCa搭載携帯電話
  - ・FCF/FCFキャンパスカード
- MIFARE（マイフェア）
- iKey1000※2

※1 ICカード内に読み取り可能なID情報が必要です。
※2 USBキーです。
※3 上記デバイスの情報は一例です。

SmartOn Pass

シングルサインオン（パスワード自動入力機能）

各種アプリケーションやWebサイト、VPNクライアント、Lotus Notesなど複数のパスワードを1枚のICカードで管理し、自動入力します。パスワードを管理者が一元管理できるので、パスワードが外に漏れる事もありません。管理者にパスワード忘れ等の問合せが来る事も無くなります。利用者もパスワードを1つ覚えておくだけで良く、SmartOnで確実な本人認証を行った後のシングルサインオンなら、なりすましによる各資源の悪用も防げます。

SmartOn Desktop

PC資源のアクセス制御・利用制限

CDドライブやUSBメモリの利用禁止、アプリケーションの利用可否などのアクセス制御を行えます。コントロールパネルなど、PC機能の制限もできるので、ユーザーが誤って設定変更してしまうことも防げます。

“ホワイトリスト機能” により、利用許可アプリの事前指定が可能

利用を許可するアプリのみを設定

- ○ Word.exe（ワード）
- ○ Excel.exe（エクセル）
- ○ Gyomu.exe（社内業務ソフト）

…業務上許可されたものは使える

他のソフトはすべて使えない！

1. 「使用禁止ソフト」を次から次へと設定しなくてもよい
2. 利用制限の設定し忘れがほとんどない
3. 勝手にアプリケーションをインストールしても使えない

SmartOn デバイス制御（Option）

指定USBメモリの利用制限も可能

「会社で許可されたUSBはOK、私物のUSBはNG」という制御がユーザー単位で可能です。ICカードでユーザーを識別しているので、PCを変えても同じ制御がかかります。

● 運用例

SmartOn Crypt

ファイル・フォルダの暗号化

重要なファイルやフォルダを暗号化して安全に情報のやり取りを行うことができます。

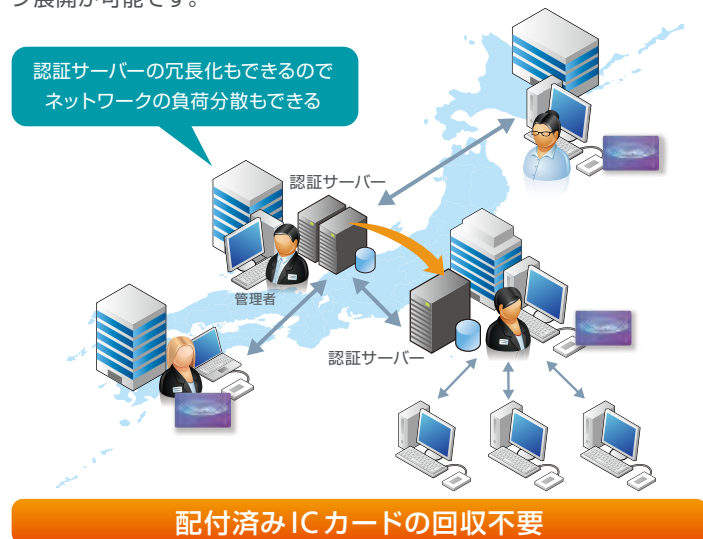
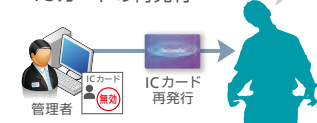
運用に配慮した管理機能

導入・運用の負荷を軽減

小規模でのスタートはもちろん、管理者権限の分散・委譲により、大規模環境にも導入可能です。各拠点でICカード管理や、ユーザー自身でICカードを登録させる事ができ、配付済みICカードの回収も必要ありません。クライアントの導入もサイレントインストールやマスターイメージ展開が可能です。

認証サーバーの冗長化もできるので
ネットワークの負荷分散もできる

認証サーバー
管理者
認証サーバー

配付済みICカードの回収不要

二要素認証にする際の課題になるカードの展開や運用、クライアントの管理もストレスを感じずに行えます。
パスワードとは違い、ICカードは紛失した事に気付きやすく、即座にICカードを失効させる事ができます。

■ クライアントの管理
- 遠隔アップデート機能
- 外出時もキャッシュでログオン可能

■ ICカードの情報変更
- 遠隔地でもサーバーで一括管理
- インポート・エクスポート機能

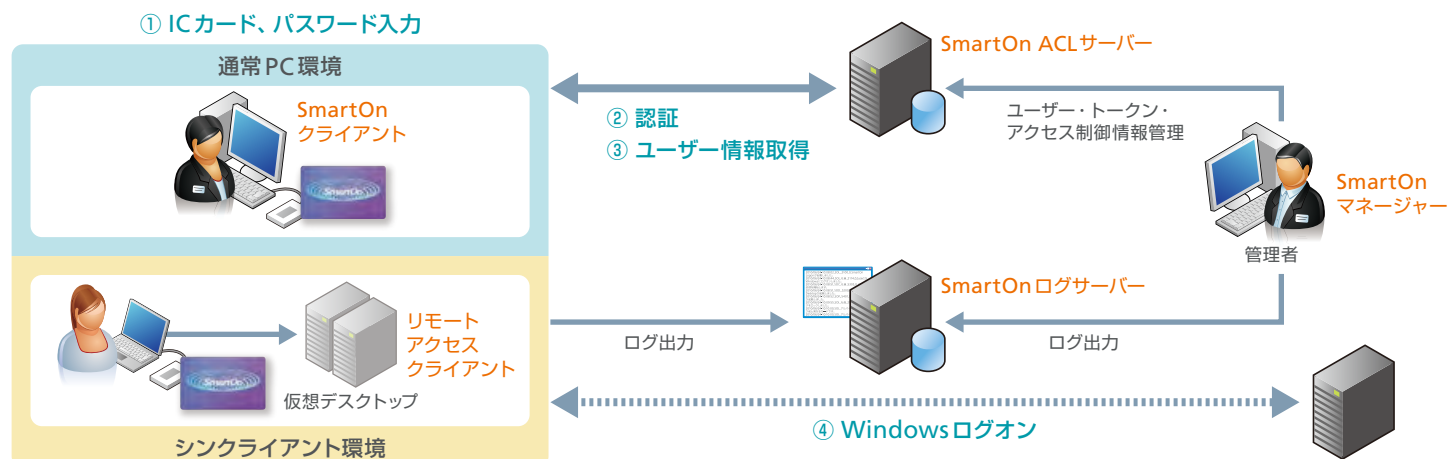
PC利用状況のログ管理

ICカードで本人を特定しているので、確実に「誰が」「いつ」PCを利用したのか、ログをサーバーで一元管理します。

● 記録する内容
- ・ログオン、ログオフ、PCロック履歴
- ・暗号化、復号化したファイル名
- ・SmartOnパスワードなどの変更履歴
- ・パスワード自動送出履歴
- ・マネージャーの操作ログ（変更、追加、削除等）

● SmartOnログサンプル

2014/04/10-08:48:02,SOL,5100,0,SmartOn Logonが起動しました。
2014/04/10-08:48:44,SOL,fukushi,2004,0, [yfukushi] がWindowsにログオンしました。
2014/04/10-12:09:26,SOL,fukushi,2150,0,コンピュータをロックしました。
2014/04/10-12:10:15,SOL,ehara,2100,0,ロック前と異なるカードです。
2014/04/10-12:10:15,SOL,ehara,2171,0,コンピュータのロックを解除しました。
2014/04/10-12:40:02,SOL,ehara,2150,0,コンピュータをロックしました。
2014/04/10-12:58:05,SOL,fukushi,2100,0,ロック前と異なるカードです。

構成概要（SmartOn ID / SmartOn ID for リモートアクセス）

通常PC環境・シンクライアント環境の混在でも運用可能です。

上の図中にある色分けは右記の通りです。 ■橙字・・・製品コンポーネント ■緑字（数字付き）・・・SmartOn認証の流れ

SmartOn連携ソリューション

InfoTrace PLUS, NetAttest BigData

PC上のあらゆる操作を記録、分析

SmartOnとPC上の操作ログを取得する「InfoTrace PLUS」を組み合わせることで、「誰が」「いつ」「何をしたのか」を確実に把握することができます※。
また、統合ログ分析アプライアンス「NetAttest BigData」を利用すれば、グラフや表などわかりやすいレポートで、よりスピーディな状況把握が可能になります。複数システムのログも統合的に分析できます。

※記録可能な操作ログは利用環境等にも依存します。

● InfoTrace PLUSログサンプル

いつ	どのデータを	どのデバイスに		何をしたか	誰が		どのPCから	
日付	ファイル名	新しいデバイス	新しいファイル名	イベント	ログオンユーザー名	SmartOnユーザー名	コンピュータ	IPアドレス
2014/4/10	¥¥fileserver¥顧客情報.xlsx	REMOVABLEDISK	E:¥顧客情報.xlsx	COPY	tsoliton	ソリトン　太郎	sales03	192.168.1.100

● NetAttest BigDataレポートサンプル

▲認証状況の概要把握

詳細情報の確認 ▶

認証成功件数の推移や、不使用トークン数など利用状況が一目瞭然、ドリルダウンで詳細情報を確認できます。

Soliton SecureBrowser, Soliton SecureGateway

スマートデバイスでもシングルサインオン

マルチデバイス対応のセキュアアクセスソリューション「Soliton SecureBrowser / Soliton SecureGateway」との連携により、PC同様にスマートデバイスでもシングルサインオン機能を利用することができます※。

※スマートデバイスからのシングルサインオンは、Webフォーム認証のみに対応します。

スマートデバイスを業務に利用しているが、Webサイトごとの認証が面倒・・・

SmartOnを使用しているPCと同様に、スマートデバイスでもシングルサインオン機能が利用できます。各WebサイトごとにID・パスワードを入力する必要がなくなります。

スマートデバイスで臨時パスワード発行

スマートデバイスから代用コード（臨時パスワード）の発行も可能です。ICカードを忘れたユーザーから至急の対応依頼も自席に戻らず迅速に対応することができます。管理者は各ユーザーの代用コードを発行でき、代用コードの有効期限や使用回数も指定できます。

SmartOnシリーズラインナップ ● SmartOnシリーズは、お客様のご利用目的に合わせて3製品ご用意しています。

	SmartOn ID	SmartOn ID for リモートアクセス	SmartOn NEO
Logon（ログオン）	●	●	●
Desktop（デスクトップ）	●	—	●
Pass（パス）	●	●	●
LogServer（ログサーバー）	●	●	●
デバイス制御	●※1	—	●※1
Crypt（クリプト）	●	—	●
認証サーバー	必要	必要	必要
ユーザー情報の集中管理	●	●	●
ICカードへの書き込み	不要	不要	必要
仮想デスクトップ対応	—	●※2	—

動作環境

ACLサーバー	Windows Server 2003/2003R2/2008/2008 R2/2012/2012 R2		
ログサーバー	Windows Server 2003/2003R2/2008/2008 R2/2012/2012 R2		
マネージャー	Windows Server 2003/2003R2/2008/2008 R2/2012/2012 R2 Windows XP/Vista/7/8/8.1		
クライアント	Windows XP/Vista/7/8/8.1	Windows Server 2003/2003 R2/2008/2008 R2/2012/2012 R2 Windows XP/Vista/7/8/8.1	Windows XP/Vista/7/8/8.1

主な対応認証デバイス

認証トークン			
FeliCa	○	○	○
MIFARE	○	○	—
iKey 1000 8KB	○	—	○
ICカードリーダーライタ			
ACS製ACR122※3	○	○	—
ソニー製RC-S330/S※4	○	—	○

※1 オプション機能です。 ※2 Citrix XenDesktop/XenApp、VMware Horizon View、Microsoft VDIに対応 ※3 FeliCa、MIFAREに対応 ※4 FeliCaに対応 ※5 他にも対応認証デバイスがございます。別途お問い合わせください。

価格（税抜）

SmartOn ID	SmartOn ID for リモートアクセス	SmartOn NEO
サーバー・基本パック		
● サーバーパック 720,000円 ● サーバーコンパクトパック 180,000円	● サーバーパック 720,000円 ● 拡張マネージャーパック 180,000円	● サーバーパック 960,000円
クライアントライセンス		
● PCインストールライセンス ～10,000円/PC ● アクティブトークンライセンス 700円/認証トークン	● リモートアクセスクライアントライセンス ～15,000円/仮想デスクトップ数または同時アクセス数 ● アクティブトークンライセンス 700円/認証トークン	● PCインストールライセンス ～12,000円/PC ● アクティブトークンライセンス 700円/認証トークン

⚠ 安全に関するご注意	正しく安全にお使いいただくために、ご使用の前に必ず「取扱説明書」をお読みください。

株式会社ソリトンシステムズ http://www.soliton.co.jp
〒160-0022 東京都新宿区新宿 2-4-3
TEL 03-5360-3811 FAX 03-5360-3880 netsales@soliton.co.jp
大阪営業所 06-6821-6777 福岡営業所 092-263-0400
名古屋営業所 052-963-9700 東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは2014年4月現在のものです。仕様、デザイン、価格は予告なく変更することがあります。 SO-1404A